SOFTWARE
RELEASE NOTES

CT-5364A-A431-312CTU-C03_R01

May 31, 2011

Introduction

The purpose of this document is to announce the general availability of software version CT-5364A-A431-312CTU-C03_R01 for model CT-5364A.

Revision Summary

Software Version	DSP/DSL Line Driver	CFE Version	Wireless Version	Release Date
A431-312CTU-C03_R01	A2pB025c1/d20l	1.0.37-12.1-24	4.174.64.12.cpe1.1	5/31/2011
A431-312CTU-C02_R08	A2pB025c1/d20l	1.0.37-12.1-15	4.174.64.12.cpe1.1	1/23/2011
A431-312CTU-C01_R02	A2pB025c1/d20l	1.0.37-12.1-15	4.174.64.12.cpe1.1	9/11/2009

New Features

- IP Address Mapping (Static NAT)
- Configurable TR-069 identifier: MAC or Serial Number (MAC is default)
- Reset-to-default/CFE recovery timers and behavior changed as follows:
  1. Hold down reset button for 10 seconds to reset to defaults
  a. Once activated, Internet, ADSL, and Power LEDs shall simultaneously flash for 5 seconds at 2Hz duty-cycle
  2. Hold down reset button for 60 seconds to activate CFE recovery mode (firmware recovery mode).
  a. Once activated, POWER LED shall flash for 5 seconds with a 4Hz duty-cycle and then illuminate steady red. All other LEDs shall be turned off at the moment of activation and until reboot begins (LAN LED will remain on if connected).
  b. Successfully uploading a binary image file from CFE recovery mode shall erase the existing configuration and replace it with the config within the binary image file (configurations saved using the savedefault.html feature will be erased)
- Configurable User Accounts/Privileges (support and user accounts are now disabled by default)
- Added ‘XBOX Live’ option to Port Forwarding and Port Triggering menus
- Support CLI configuration of TR-069 client

Changes and Fixes

- Set minimum allowed TR-069 Inform Interval to be 300 seconds
- Fixed memory leak issue
- Added various security enhancements to web GUI and CLI
- Fixed Guest SSID not being isolated from wired LAN
- Fixed LAN DHCP timeout issue
- Changed Rekey interval from 0 to 3600 and encryption from AES to TKIP+AES

Anomalies

- Interface Grouping (Port Mapping) doesn't automatically revert to default if Advanced DMZ is enabled then disabled. This can be done manually in the Interface Group menu
- Wi-Fi Protected Setup (WPS) – PBC and PIN method could fail intermittently
- When Wi-Fi authentication 'None' is selected, wireless still shows enabled in GUI
- Guest SSIDs are functional only when wireless security is 'Open'
- TR-069 may stop checking in after a few days uptime with MER WAN
- Vendor ID in Interface Group can't be edited. It must be removed and reconfigured
- When the firewall is disabled, the modem replies to WAN pings even though ICMP is disabled in the Access Control menu
- Manual selection of 100HD/FD and 10HD/FD not working on LAN ports 2 and 4

Compatibility/System Notes

This version is backwards compatible with all previous versions listed above in the revision summary.

Advanced DMZ is a feature which permits the modem's WAN IP address to bypass NAT and automatically get port mapped directly to LAN port 4. A DHCP client connected to this port will share the modem's WAN IP address. The shared WAN IP is also NAT'ed to LAN ports 1-3 to offer traditional private IP addresses to connected LAN devices. When configuring Advanced DMZ it's necessary to specify the non-DMZ subnet. This will be the DHCP LAN subnet supplied to devices attached to LAN ports 1-3 and also becomes the subnet to locally manage the modem from those ports. The IP configured in Advanced Setup/LAN is the local management address for LAN port 4. NAT and Port Mapping menus will disappear when Advanced DMZ is configured. Advanced DMZ is configured in the Advanced Setup/WAN menu during the process of creating a routed WAN interface.

This release supports Physical Layer Retransmission (PhyR) which operates at layer 1 and uses a mechanism similar to TCP where retransmits occur if errors are detected. This results in high effective impulse noise protection with minimal interleave delay. Sync rate increases from 2 to 4Mbps have been reported in addition to the line being more robust and resistant to noise from treadmills, ceiling fans and lightning. PhyR is not configured on the modem but is negotiated automatically during the initialization process with the DSLAM (this is Broadcom proprietary). Versions supporting PhyR can be identified by the number 3 in the third character of the file name (A431-312CTU-C02_R08).

IGMP Snooping Definitions:
Standard Mode - in standard mode, if multicast traffic is present on a LAN port but no membership report (join) was received, the traffic will flood to all ports. If a membership report was received, multicast traffic will be forwarded only to the LAN ports on which the IGMP membership reports arrived.
Blocking Mode - in blocking mode, multicast traffic will be blocked from all ports until such time a report is received.

In both modes the modem will monitor IGMP activity from each multicast group (channel) and remove the group from its forwarding table if none is detected for 150 seconds. Video tiling can occur if the DSLAM query period is longer than 150 seconds.
Enhanced IGMP – the purpose of enhanced mode is to prevent STBs from receiving IGMP reports from other LAN-attached STBs so as to ensure they'll always send IGMP report and leave packets even if watching the same channel.
If IGMP snooping is disabled the switch floods multicast packets to all its ports.

MAC address considerations - Each modem contains a label indicating its LAN (base) MAC address. The source MAC address contained in upstream packets equals this address +1 for Ethernet WAN and +4 for DSL WAN (PVC). Example: unit with a base MAC ending in AA:10 will assign AA:11 to its Ethernet WAN or AA:15 to its 1st PVC. Additional WAN interfaces will increment by one. In the case of TR-069, the modem's base MAC address will be used.

Wireless is enabled by default with SSID Comtrendxxxx (x = last four characters of base MAC). Wireless security is WPA2-PSK passphrase = last ten of base MAC address. Rekey interval = 3600 and encryption = TKIP+AES

Static NAT definitions:

ILA: Inside Local Address
IGA: Inside Global Address

One-to-One: one ILA is mapped to one IGA
Many-to-One: multiple ILAs are mapped to one IGA (aka PAT)
Many-to-Many: each ILA is mapped to a unique IGA
Many-to-Many (with overload): multiple ILAs are mapped to shared IGAs

Port Mirroring – is a troubleshooting/debugging aid which makes it possible to monitor WAN traffic from the LAN using Wireshark or other tools. Incoming and outgoing traffic can be monitored separately or simultaneously. This feature is accessed at 192.168.1.1/engdebug.cmd. For more information on using this feature contact your Comtrend rep.

Historical

A431-312CTU-C02_R08

- NAT Loopback – This feature allows for an internal IP address to be accessed via its public (external) IP address or domain name. Packets are subjected to normal WAN filtering rules
- MAC Cloning
- Added Home button to savedefault.html menu
- Added PhyR status to ADSL statistics page
- Added or verified standard North American features including;

- Firewall checkbox
- Enhanced IGMP mode
- "PPPoE debug mode" - disabled by default
- “Bridge PPPoE frames between WAN and LAN ports” option in GUI and disabled by default
- Added several TR-069/ACS enhancements and resolved several anomalies
- Added ‘None’ option for Wi-Fi authentication
- Support configurable MTU (64-1492 for PPPoE and 64-1500 for PPPoA)
- “Enable NAT” option in PPP GUI and enable it by default
- Support DHCP option 121
- Admin privileges for remote access
- ACL configuration allows entries for source IP/Mask and Interface
- Telnet/SSH logout command
- Enable FTP/TFTP on LAN side by default
- PPPoE discover packet sent continuously until it authenticates
- Renamed Save/Apply to Apply in DSL menu
- LAN MAC = MAC on sticker = TR-069 MAC = SSID/WPA2 MAC
- traceroute command in CLI
- Gratuitous ARP - In cases where the modem contains a static IP (i.e.; MER), this feature generates traffic enabling upstream equipment to populate its MAC table
- SIP ALG
- TR-069 - when CPE reports to ACS, changed manufacturer name from Broadcom to Comtrend and model name from board ID to Comtrend model name/number
- Support SNMP
- DNS relay supported by default
- Device Info page shows full CFE version and serial number
- Ethernet Media Type function
- ifconfig command in CLI
- Adjust Wi-Fi transmit output power to 17dBm by default
- apuser account (username/password = apuser/apuser)
- save default feature
- Changed DHCP option 60 vendor ID from universal “uDHCP 0.9.6” to reflect the model, “Comtrend CT-5364A”
- Support HTTP redirect by enabling "Retry PPP password on authentication error"
- Expanded the number of special characters that can be used for the PPP password ("`~^()_|;'<>#$&*\-!@%=+[]/.,{})
- Added support for “brctl” commands in CLI. “brctl” is a bridge administration utility used to inspect bridge configurations. It can be used to see MAC address to bridge interface associations. To use this feature, telnet to the unit, log in and type “brctl show”
- Advanced DMZ

- Disable UPnP by default
- Resolved CPE failing to renew DHCP leases then denying access to the WAN
- Fixed URL filter feature
- Added TR-069 KeyPassphrase parameter
- TR-069/default config parameter

- Fixed unable to configure URL filter using Firefox
- Fixed allow MAC address feature
- Fixed remote SSH issue using “root” account
- ADSL LED is now off when ETH WAN is configured
- Resolved WAN Auto-detect feature with DSL + DHCP (MER)
- Fixed Internet LED behavior in Ethernet WAN mode
- Changed that upon power up the modem no longer acts as a bridge prior to the Ethernet WAN being initialized
- Fixed DHCP discover unexpectedly sent while IP is maintained
- Added pop-up warning when enabling allow MAC feature to remind user to add local management PC
- Xbox Live fix
- Changed wireless bandwidth from 40MHz in both bands to 20MHz in 2.4G band
- Resolved WAN MAC becoming 02:10:18:10:10:01
- Default wireless security is now WPA2-PSK, passphrase = last ten of base MAC address. Rekey interval = 0 and encryption = AES
- Fixed PPP extension mode when coexisting with Bridge and MER
- Fixed issue with DHCP and ARP after power cycle in ETH WAN mode
- Added base MAC address to syslog messages
- Resolved DSL retrain causing default gateway to be deleted
- Resolved default gateway not getting updated after DHCP server change and line retrain
- Added ability to edit ETH WAN interfaces
- Support Bridge mode and 802.11p/q for ETH WAN
- Fixed modem reporting incorrect uptime to ACS
- 802.1q VLAN tag support
- Resolved intermittent issue of modem becoming unresponsive
- Fixed IGMP Proxy not working with 2 routed PVCs configured
- Fixed PPP debug log disabling after save/reboot
- Fixed issue with accessing GUI after changing login password
- Fixed LAN FTP access issue where FTP didn’t work after disable/re-enable
- Removed “Display SOAP messages” option from GUI
- Fixed issue where some WAN interfaces would get disabled if hitting Save/Apply too soon after checking “Enable Virtual Ports”
- Fixed TR-069 beacon advertisement enabled was not applied to main SSID but only Guest SSID
- Fixed TR-069 incorrectly reported host table
- Support TR-098 parameters:

・ WLANConfiguration.1.BeaconType
・ WLANConfiguration.1.BeaconAdvertisementEnabled
・ Diagnostic Ping without being told explicitly what interface to ping from
・ Active Notification
・ WLANConfiguration.1.SSID - Can be set by the ACS. CPE must be rebooted to apply
・ WLANConfiguration.1.BasicEncryptionModes
・ WLANConfiguration.1.WEPKey.1.WEPKey
・ WANIPConnection.Uptime
・ In the datamodel the CPE lists the interface type for connected wireless hosts as Wi-Fi

A431-312CTU-C01_R02

- WAN Interface Auto Detection – this feature (which is enabled by default) will auto-detect the WAN interface type (DSL or Ethernet) and automatically configure the interface for IPoE or RFC1483. In this version, PPPoE/A requires manual intervention
- Custom Default Configuration – this feature allows the user to create unique factory default settings on a per modem basis and, if desired, to upload those settings onto other modems for the same purpose. If the modem is factory defaulted it will default to the settings that were saved using this process. The menu for this feature is accessed at http://192.168.1.1/savedefault.html which also includes a detailed description
- The DHCP vendor ID field within the port mapping menu now supports special character entries such as !@#$%^&*()
- Added a TR-069 VLAN MUX (802.1q) parameter
- IGMP version is now selectable (V2/V3) in the Advanced Setup/LAN menu. This setting pertains to IGMP Proxy (WAN) in router-mode
- Added WPS (Wi-Fi Protected Setup) which supports both PIN and Push Button methods
- Bits per Tone Graph - This feature is located in the Device Info/Statistics/ADSL menu, at the bottom of the page, and is called "Draw Tone Graph". The graph provides a general representation of bit allocation across the spectrum. More details can be seen by telneting into the modem and typing "adsl info --Bits" where a list of all 255 tones and associated bits can be seen
- Save Default configuration - This feature allows the user to manually create unique factory default settings on a per-modem basis. This is accomplished by simply using the modem's GUI as usual to create the desired configuration then, after a save and reboot, telneting to the modem and issuing a save command as follows; *save_default --save* (space between default and the two dashes). After this point, if the modem is factory defaulted using the rear-panel reset button or via the menu's restore default command, the modem will default to the settings that were saved using this process. There are also commands for clearing and reading the default settings; *save_default --clear, save_default –read*
- Gratuitous ARP - in cases where the modem contains a static IP (i.e.; MER), this feature generates traffic enabling upstream equipment to populate its MAC table
- The backup configuration filename has been changed from backupsettings.conf to *version_name*.conf. The name of the backup file will reflect the software revision resident on the modem (example: A101-310CTU-C01_R02.conf). The file name can be modified but should be preserved if the need arises to email it to Comtrend
- A new modem management privilege level has been added. This is in addition to Root, Support and User. This new level is called "apuser" and restricts menu access to changing the Wi-Fi settings, NAT, Parental Controls, running diagnostics, viewing statistics and Save/Reboot. This restricted GUI is accessed with the user name and password "apuser"
- Added Full Cone NAT support

- TR-069 field InternetGatewayDevice.DeviceInfo.ModelName now shows actual model name instead of board ID
- Support extra characters that can be used for the PPP password
- Modem reports the most recent 32K of its system log to an ACS
- TR-069 enhancements including ClearAccess patches
- NAT is enabled by default for PPP connections
- SSID up to 20 characters
- Fixed that "Save/Apply" button in Interface Group would disable LAN interfaces
- Corrected GUI ADSL Statistics output power values - downstream and upstream were reversed
- Fixed adding a second vendor ID caused the port mapping menu to delete the first one
- Modified “user” account to support only the following menus; NAT, Parental Controls, Wireless/all, Statistics, Device Info, Diagnostics, Save/Reboot

UPGRADE PROCEDURE

A special upgrade procedure is required if upgrading from 4.02 to 4.06-based versions. Please contact your Comtrend rep for upgrade instructions.

1. **Upgrade Software**
    a. Open a web browser, connect to 192.168.1.1, and login with username **root** and password **12345** (or appropriate IP address and login info)
    b. Click Management→Update Software and select the Browse button
    c. Locate and double click on the appropriate Comtrend software image
    d. Select the Update Software button. The software image will be uploaded to the modem and the modem will reboot automatically upon completion
2. **Restore to Default**
    a. Hit the F5 Key to refresh your browser and reconnect to 192.168.1.1 to log back into the modem
    b. Click on the Management link
        I. Click on Settings
        II. Click on Restore Default
        III. Click the Restore Default Settings
3. **Verify**
    a. Hit the F5 Key to refresh your browser and reconnect to 192.168.1.1 to log back into the modem
    b. Click on Device Info
    c. Verify that the latest code is shown in the Software Version field: A431-312CTU-C03_R01.A2pB025c1.d20l
4. Upgrade and verification procedure is complete!

TECHNICAL SUPPORT

For technical support contact your Sales Engineer or Comtrend Technical Support at 949-753-9640, Option 3. You can also submit questions and comments at http://www.comtrend.com/na/contact.htm

RMA REQUEST

An RMA can be initiated at http://customersupport.comtrend.com/

The contents of this document are current as of the date of publication. Comtrend Corporation reserves the right to change the contents without prior notice. In no event will Comtrend Corporation be liable for any damages or for commercial losses resulting from information contained in this document.

Comtrend Corporation
16 Goodyear, Suite 120
Irvine, CA 92618
(949) 753-9640